(12) UK Patent Application (19) GB (11) 2 349 244 (13) A

(43) Date of A Publication 25.10.2000

(21) Application No 9909159.7

(22) Date of Filing 22.04.1999

(71) Applicant(s)
Visage Developments Limited
(Incorporated in the United Kingdom)
Mayfield, Old Malden Lane, WORCESTER PARK,
Surrey, KT4 7PU, United Kingdom

(72) Inventor(s)
Paul Barrett
Andrew Ryan

(74) Agent and/or Address for Service
Urquhart-Dykes & Lord
1 Richfield Place, Richfield Avenue, READING,
RG1 8EQ, United Kingdom

(51) INT CL[7]
G06F 1/00 12/14

(52) UK CL (Edition R)
G4A AAP

(56) Documents Cited
EP 0447339 A2 EP 0442839 A2 EP 0442838 A2
WO 97/15008 A1

(58) Field of Search
UK CL (Edition Q) G4A AAP
INT CL[6] G06F

(54) Abstract Title
Providing network access to restricted resources

(57) A distributed client/server computer system comprises a network of servers and clients, such as the Internet, in which user access to certain restricted resources administered by some servers is controlled by a logon procedure that identifies an authorised user to the respective administering server. The system includes a logon server accessible by clients, and the logon server is provided with:

a) a user authentication procedure by which a user can log on to the logon server from any client and uniquely identify that user to the logon server;

b) a stored library, specific to a user of the logon server, of network addresses of user-selected resources, including restricted resources, and of user data to satisfy logon procedures for the user to access the restricted resources; and

c) means for detecting a request from a logged-in user through a given client for access to data from a resource, and, in the case of a restricted resource, for then carrying out at least one of the following procedures:

(i) using the stored library to complete a user logon procedure, receiving the requested data from the server administering the resource, and forwarding the data to the client;

(ii) using the stored library to prepare a user logon form and forwarding the form to the client by which it was requested, for the user to submit to the resource to log the user on to that resource;

(iii) using the stored library of user data to partially complete a user logon form for that resource on behalf of the user, serving the partially complete form to the client, receiving the form from the client after the insertion of data by the user, and adding data inserted into the form by the user to the library for recall for future use in procedure (i) or (ii).

The logon server in effect maintains a library of usernames and passwords for the selected restricted web sites chosen by each user and automatically logs the user on to them when selected by the user from a personal catalogue held by the logon server.

GB 2 349 244 A

SYSTEM AND METHOD FOR PROVIDING NETWORK ACCESS TO RESTRICTED RESOURCES

FIELD OF THE INVENTION

The present invention relates to a system and method for providing network access to restricted resources. The following description will explain the invention in terms of the Internet or an intranet, but the invention is not so limited in principle and can be applied to any suitable network of distributed client and server computers.

BACKGROUND OF THE INVENTION

The Internet is well known. It is a network of computers multiply linked together, using a set of network protocols known as Transmission Control Protocol/Internet Protocol (TCP/IP). According to these protocols, computers connected to the Internet are assigned IP addresses, which for convenience are also identified with domain names. These domain names are referred to in Uniform Resource Locators (URLs) by which files, or pages, are identified on the worldwide web. A web site is typically defined as a set of network addresses on the World Wide Web under a single second level domain name. Domain name servers exist to translate requests for network access to a URL by an Internet client into the corresponding IP address. Access to web pages is normally carried out through a browser on the client machine which enables a user to enter a URL, and when the browser is given the submit command the browser should retrieve the corresponding file or page from the appropriate server on the Internet. The client computer may be connected to the Internet through the server of an Internet access provider, which may include a proxy server at which frequently accessed web pages are stored for faster retrieval by the client.

Web pages are written in HyperText Markup Language (HTML), and transmitted across the Internet by means of HyperText Transfer Protocol (HTTP). Resources on a network are often protected by passwords, and resources on the Internet are no exception. For example, a web site may simply wish to identify those who access it for statistical purposes, or for commercial purposes, or certain sites may simply be

private, or certain sites may only be accessible by payment of a fee in which case user identification is required for billing purposes. Typically, restricted web resources identify users by means of a username and password combination. The username is generally a name or word known openly, and is used for identifying the user, while the password is some other word or phrase or combination of symbols that need be known only to the server administering the resource and to the user. Provided that the password submitted by the user matches the password stored against the username by the resource-administering server, access is permitted.

Accordingly, in order to obtain access to a restricted resource, it is first necessary for a prospective user to go through an enrolment procedure, in which a convenient username is recorded against the necessary details, such as name and address and account number, of the user, and then the user enters a secret password which is recorded by the resource server against the username. On subsequent visits to the restricted site, the user then completes an authentication procedure, which on the worldwide web typically involves an HTML logon form by means of which at least the username and password are submitted to the administering server. Once access has been provided in a browser session, further requests for data from the restricted resource by the user can be assured by the use of known procedures such as Basic Authentication or the use of persistent client state objects (cookies).

There are also restricted resources (resources requiring a username and logon procedure) which do not require a pre-arranged password, and those that do not require any password at all. Access to these restricted resources is also within the purview of this invention. A simple enrolment procedure with an acceptable username may be all that is required.

As is also well known, modern web browsers include such features as bookmarks, or favourites, or hotlists. These can take the form of a file, or hypertext page, with links to destination URLs that have been deliberately selected and stored by the user. By clicking on a name, button or link in this catalogue, using a browser and a pointing device such as a mouse, a user can cause the browser to fetch the appropriate page from the Internet and display it. If the page is one that requires user authentication, because the resource is restricted, the user is required to use the appropriate access procedure, in the course of which the correct username and password must typically be provided. For security reasons, it is advisable to use

different passwords for different resources, and usernames may well also be different. The user therefore has the task of remembering or conveniently recording (even though this is a poor security practice) this information, often in the browser or elsewhere on the user's Internet client computer.

SUMMARY OF THE INVENTION

The present invention provides a logon server on a distributed client/server network in order to simplify user logon procedures.

The logon server is used to implement a web-based service that provides a centralised repository for users' favourite destinations which can be stored in a library of user-specific and general resource data and displayed to the user as a catalogue of selectable resources. Unlike other similar web based services, the logon server also provides a mechanism for web based single sign on to sites that require entry of a username or password (or any other user specific information).

In accordance with one embodiment of the invention there is provided a distributed client/server computer system comprising a network of servers and clients in which user access to restricted resources administered by at least some of said servers is controlled by a logon procedure that identifies an authorised user to the respective administering server, which system includes a logon server accessible by a plurality of clients, and the logon server is provided with:

a) a user authentication procedure by means of which a user can log on to the logon server from one of said plurality of clients and use said authentication procedure to uniquely identify that user to the logon server;

b) a stored library, specific to a user of the logon server, of network addresses of user-selected resources, including restricted resources, and of user data to satisfy logon procedures for the user to access the restricted resources; and

c) means for detecting a request from a logged-in user through a given client for access to data from a resource, and, in the case of a restricted resource, for then carrying our at least one of the following procedures:

(i) using the stored library of user data to complete a user logon procedure for that resource on behalf of the user to log the user on to the resource, receiving the requested data from the server

administering the resource, and forwarding the said data to the client by which it was requested;

(ii) using the stored library of user data to prepare a user logon form for that resource on behalf of the user and forwarding the said form to the client by which it was requested for the user to submit to that resource to log the user on to that resource;

(iii) using the stored library of user data to partially complete a user logon form for that resource on behalf of the user, serving the partially complete form to the client, receiving the form from the client after the insertion of data by the user, and adding data inserted into the form by the user to the library for recall for future use in procedure (i) or (ii).

The user logon procedure will typically be a user enrolment procedure or, on subsequent visits by the user to the resource, a user authentication procedure. Likewise the user logon form will typically be a user enrolment form or, on subsequent visits by the user to the resource, a user authentication form.

Preferably, in such a system the logon server authentication procedure includes transferring a username from the client to identify the user and transferring a verification from the client to verify the user, wherein the verification is an action specific to that username. A particularly preferred action is a demonstration of the recognition of a specific set of human faces. The security benefits of such a system, and methods of implementing it, are described in International Patent Application WO93/11511, the disclosure of which is incorporated herein by reference. The logon server may be provided with means for requesting access to the data from the server administering the resource, whereby to determine whether the resource is a restricted resource. This may comprise means for searching for an HTML form in order to determine whether the resource is a restricted resource.

The means for carrying out procedures (i), (ii) and (iii) may include a store of user logon forms for restricted resources.

The stored library may include a user-editable catalogue of resources and the logon server means may be provided with means for displaying the catalogue to the user for enabling the user to select a resource to log on to. Such a catalogue may be

specific to the user. Desirably, selection of a resource from the catalogue by the user is interpreted by the logon server as a request for access to data from that resource. The catalogue accordingly serves as a bookmark or favourites destination file that can be accessed by the user irrespective of the client that they are using at any time.

In accordance with a further embodiment of the invention there is provided, for use with a distributed client/server computer system comprising a network of servers and clients in which user access to certain restricted resources administered by at least some of said servers is controlled by a logon procedure that identifies an authorised user to the respective administering server, a method of logging a user on a to user-selected restricted resource from a user-selected one of a plurality of clients, comprising:

a) providing a logon server in the network;

b) transmitting a user request from said one client to said logon server to log the user on to the server;

c) invoking a user authentication procedure by means of which a user can log on to the logon server from one of said plurality of clients and use said authentication procedure to uniquely identify that user to the logon server;

d) maintaining a stored library, specific to a user of the logon server, of network addresses of user-selected resources, including restricted resources, and of user data to satisfy logon procedures for the user to access the restricted resources;

e) detecting a request from a logged-in user through a given client for access to data from a resource, and, in the case of a restricted resource, then carrying out at least one of the following procedures:

(i) using the stored library of user data to complete a user logon procedure for that resource on behalf of the user to log the user on to the resource, receiving the requested data from the server administering the resource, and forwarding the said data to the client by which it was requested;

(ii) using the stored library of user data to prepare a user logon form for that resource on behalf of the user and forwarding the said form to the client by which it was requested for the user to submit to that resource to log the user on to that resource;

(iii) using the stored library of user data to partially complete a user

logon form for that resource on behalf of the user, serving the partially complete form to the client, receiving the form from the client after the insertion of data by the user, and adding data inserted into the form by the user to the library for recall for future use in procedure (i) or (ii).

The same steps may be used in a method according to the invention of authenticating a client to a server in a distributed client/server computer system comprising a network of servers and clients in which user access to certain restricted resources administered by at least some of said servers is controlled by a logon procedure that identifies an authorised user to the respective administering server.

The user data from the library may be used in order to log the user on to a resource not previously accessed by the user through the logon server if the resource requests data that is already held for that user in the library.

The user may be authenticated in subsequent visits to a restricted resource by the logon server serving a completed input (logon) form either direct to the resource or to the client for the client to submit to the resource.

The following brief description sets out in outline how a user may make use of the invention. It is to be understood that this is merely an overview of a typical system according to the invention.

Firstly, the user logs on to the logon server from any client computer on the network, using an authentication procedure previously established for that user.

When the user adds a new URL to their logon server destinations, the logon server checks the corresponding web page to see if that page requests information from the user. If it does, then the logon server displays the page to the user for them to fill in. The logon server captures the details that the user fills in and will replay this information to the site when the user returns to that site via the logon server. In this manner, the logon server provides the user with a single sign on service to their favourite web destinations.

Because all of the user's destination and single sign on information is stored centrally on the logon server database, the user gains mobility - they can use their destinations, usernames and passwords etc. from any computer with web access.

Additionally, the logon server lists a number of "top sites" which can be automatically transferred to the user's destinations (without the user having to enter the URLs). For these sites an automatic enrolment feature is also offered. If the user clicks on this option, the site's enrolment form is displayed, the logon server captures the user's enrolment information (name, address, username, password and other demographic information is often requested). The logon server can use this captured information to automatically 'fill in' enrolment forms for other sites.

In this manner, the invention accelerates the user's route to enrol and to log on to their favourite sites. The more web services the user enrols for via the logon server, the more information the logon server gathers and enrolment to other web services becomes more automated.

The aforementioned and other features of the invention will become more apparent from the following more detailed description of preferred embodiments of the invention.

DESCRIPTION OF PREFERRED EMBODIMENTS

In an exemplary distributed client/server computer network system in accordance with the invention, using the Internet, many users can access the Internet in any known way using, in particular, convenient client computers to identify themselves to a logon server and to authenticate themselves by taking an action that verifies their identity. Currently, such a system involving a demonstration of the recognition of a set of human faces is demonstrated at our web site http://www.id-arts.com/ where methods disclosed in WO93/11511 are implemented.

After logon to the logon server with authentication to uniquely identify the user, there are a number of ways in which the invention is used. The user can use a single sign on procedure to add to their destinations new resources (i.e. web sites)

selected entirely by themselves, or they can use an automated enrolment procedure to add sites specifically offered by the logon server. In each case, there is an initial enrolment phase, followed by simple authentication on subsequent visits to the same site.

Example 1 - Single Sign On

The term 'single sign on' is used herein to mean a service offered by the logon server by which an authorised user of multiple restricted resources listed in the user's catalogue only has to make one single sign on in a browser session in order to access any of those resources. That sign on is the user's sign on, or logon, to the logon server itself. Signing on or logging on to the catalogued resources, including username and password submission, is thereafter handled automatically by the logon server.

The following description concerns firstly the initial procedure of adding a new resource to the user's catalogue.

When the user enters, by means of their browser, the network address (conveniently, as the URL) of the resource that they wish to add to their catalogue of destinations, the logon server reads that page (via its proxy server). Using procedures that will be understood by those skilled in the art, the logon server looks for an HTML form within that page and, if it finds one, it offers the users a check box to enable single sign on for that service.

If the user chooses to use single sign on, the logon server rewrites the HTML of the page that the user has requested to ensure that:

- All HREFS are removed so that no links can be followed off the page;
- All image tags are rewritten to ensure that their URLs are absolute and so will be resolved correctly;
- The form action is rewritten to submit the request to the logon server so that the logon server will receive the input from this form;
- The original form action is added to the form as a hidden input field in order that the logon server can record where the form contents should be sent in order to achieve single sign on;

- Any input buttons are removed or converted into a single submit button (if there is not already an explicit type=submit on the page). This ensures that there is only one exit from the form and that it takes the user back to the logon server.

This rewritten page is then served to the user within a frameset that makes it clear to the user that the data that they are entering will be submitted to the logon server.

When the user enters the form, the logon server will receive the form data and can store it for the user in a library, specific to that user, containing the network address of the resource as well as the form data to satisfy the log-on procedures for the resource. The library stores a catalogue of those resources that user has chosen to include, which can be displayed to the user as the user chooses, in the manner of a hotlist.

When the user returns to their catalogue of destinations within the logon server, the logon server serves them a page that contains their destinations' input forms with all of the form contents as hidden fields. Clicking on the 'go' button for that destination will effect single sign on to the site (as the form action no longer sends the data to the logon server but to the URL contained in the original form action). In this way, the user only needs to carry out one single manual sign on procedure to access the logon server, after which the logon server handles automatically the subsequent logons to restricted sites in the user's catalogue.

Example 2 - Single Sign On within Frames

An additional complication, which requires the single sign on procedure of Example 1 to be modified, is when the form to be entered is contained with an HTML frameset. To find this form, the logon server needs to recursively search the frameset. Once it has found the frame containing a form, the logon server will serve the frameset to the user with all frame references and image references rewritten to be absolute so that they are sourced from the original site and with all HREFs removed. In effect, HREFs are HTML links to other URLs. Within this frameset, each frame reference on the route to the frame that contains the form is rewritten by the logon server in order that it will be sourced from the logon server

which will have cached these pages under their URLs. The frame containing the form will be sourced from the logon server which will rewrite it as described above.

Consequently, as in the example without frames, the user sees a composite page that looks almost identical to the log on page of the original site. The only differences are that the form data will be sent to the logon server and that there is an additional logon server frame to remind the user of this fact.

When the user clicks on the 'go' button in their catalogue next to a destination which involves a frameset, the logon server will read the top level page and all constituent frames which are on the route to the frame containing the form through its proxy server. It will rewrite them as described above and serve them to the user as above, except that this time HREFs will be made absolute rather than removed. This time, however, instead of presenting the frame containing the form rewritten to send its data to the logon server, the form is rewritten to send the user's log-on data to the original form action URL. The effect of this is that the logon server has filled in the form for the user - all they have to do is press the submit button.

In an alternative, the action of the user pressing the submit button could be simulated using Javascript, if this can be handled by the user's browser.

Example 3 - Automated Enrol

The logon server will display a list of free (existing, third party) web services for which automated enrol is enabled. For each service in this list, the logon server will provide a brief textual description of what the service offers the logon server user. If the user clicks on the 'enrol' button for a particular service, the logon server will fetch the enrolment form page for the third party site via its proxy server. The logon server will rewrite the HTML for this page in a similar manner as for single sign on. The logon server will have a template for this form which will contain a mapping between the field name used on the form and the logon server's name for this information. If the logon server has already collected any of this information about the user in its library of user data, because the user has already used the automated enrol process, then it will fill in the data in the form from its database for that user according to the template. The page will then be served to the user